Fault Mechanisms Manual

LSTS

December 7, 2011

Contents

1 Introduction

This document is intended to explain how the main emergency and fault mechanisms work in DUNE.

2 Fault Mechanisms

2.1 Servo Current Fault Detection

2.1.1 Configuration

Configuration parameters for this mechanism are located in */etc/hardware/lsct/a500.ini*.

Parameter Name	Acronym	Default	Description
Current Fault Detection	CFD	false	enables or disables current fault detections.
Current Lower Threshold	CLT	0.4	lower threshold to trigger a minor current fault detection.
Current Upper Threshold	CUT	0.7	upper threshold to trigger a major current fault detection.
Maximum Lower Faults	MLF	20	maximum number of minor faults that must be exceeded before a fault detection error is thrown
Maximum Upper Faults	MUF	4	maximum number of major faults that must be exceeded before a fault detection error is thrown
Fault Time Cooldown	FTC	60.0	cooldown time after which the counters of minor and major faults are reset
Error Throw Period	ETP	20.0	cooldown time after which a current fault error can be thrown to the output

2.1.2 Description

This mecanism attempts to detect faults in the servos by reading the measurements of electric current flowing in them. The current values are constantly being read for every servo. If the current exceeds the **Current Lower Threshold** , the minor faults counter is incremented. If the current exceeds the **Current Upper Threshold** , then both minor and major fault counters will be incremented. If a **Fault Time Cooldown** amount of time passes before a fault detection is triggered, both minor and major fault counters are reset to zero. If the values in the counters exceed, respectively, the **Maximum Lower Faults** or **Maximum Upper Faults** , there will be an attempt to throw an error to the output. If the last time an error was thrown (for that same servo) was less than **Error Throw Period** seconds ago, then the error will not be thrown. If more than that has passed then the error will go to the output. Note that this is valid for each servo independently. This means that if all servos enter a fault state and errors can be thrown, you will see in the output as many errors as the number of servos in the vehicle.

2.1.3 Flowchart

Figure 2.1 depicts the flowchart of how the fault detection method works. The example covers the faults related to the lower threshold, yet the detection for the upper threshold works in the exact same way. The letter "I" represents the value of the current being read for a certain servo.

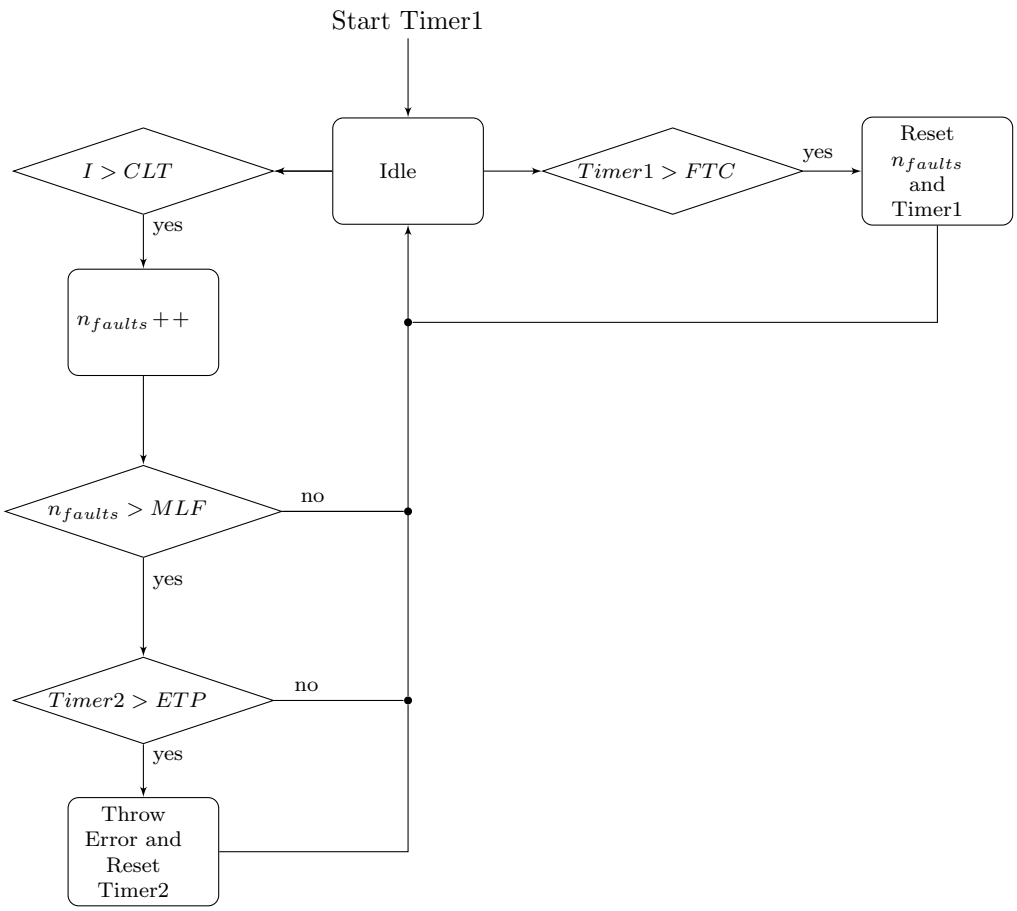

Figure 2.1: Servo current fault detection flowchart.

2.2 Servo Position Fault Detection

2.2.1 Configuration

Configuration parameters for this mechanism are located in */etc/hardware/lsct/a500.ini*.

Parameter Name	Acronym	Default	Description
Position Fault Detection	PFD	false	enables or disables position fault detections.
Position Error Threshold	PET	0.2	threshold of the error between the actuation command and servo actual position above which a detection is made.
Position Error Delay	PED	5.0	amount of time during which the position error must remain above the threshold, so that a fault detection is triggered.
Position Error Samples	PES	5	number of samples used in the moving average filtering the position error.
Error Throw Period	ETP	20.0	cooldown time after which a current fault error can be thrown to the output

2.2.2 Description

The position values of the servos (if available) are assumed to be synchronized with the command values, in other words, the adcs reading those positions are assumed to be properly calibrated. Those positions are constantly being read. The error between them and the last command sent to the servo is computed. The error value being read can be filtered with a moving average that will use **Position Error Samples** samples for that purpose. If that error goes above **Position Error Threshold** and remains above that value for more than **Position Error Delay**, a position fault error will be thrown:

> potential fault in servo #n, position error above X

The same error will only be thrown to the output again if more than **Error Throw Period** seconds have passed since the last error was thrown.

2.2.3 Flowchart

Figure 2.2 depicts the flowchart of how the fault detection method works. The variable *error* represents the absolute value of the diference between the servo's command and its actual position.

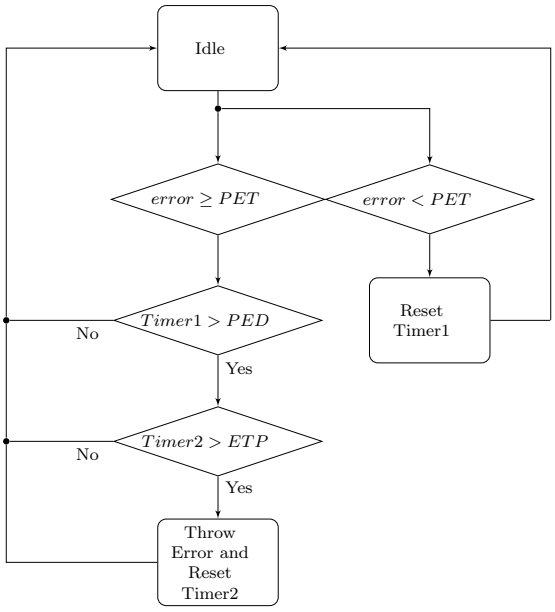

Figure 2.2: Servo position fault detection flowchart.

2.3 Motor Current Fault Detection

2.3.1 Configuration

Configuration parameters for this mechanism are located in */etc/hardware/lmct/a500.ini*.

Parameter Name	Acronym	Default	Description
Motor Current Fault Detection	MCFD	false	enables or disables position fault detections.
Motor Current Channel	MCC		ADC channel number used to measure the current. Default value depends on the MCTR version.
Motor Current Error Threshold	MCET	2.0	Threshold for the error between the motor's current and the expected current.
Motor Current Delay	MCD	5.0	amount of time during which the error must remain above the threshold, so that a fault detection is triggered.
Motor Current Average Samples	MCAS	5	number of samples used in the moving average filtering the position error.
Motor Current Error Period	MCEP	20.0	cooldown time after which a current fault error can be thrown to the output
Motor Current Interpolation Points	MCIP		curve points used to create a model of the expected motor current. No default value.

2.3.2 Description

This mechanism uses a model of the motor current versus rpms in order to assess whether or not the motor is at a fault state. That model is a piecewise linear function put together using the **Motor Current Interpolation Points**. The value of the function between each pair of points is computed using linear interpolation. *The **Motor Current Interpolation Points** are assumed to be in ascending order and in the format (rpm,current).* Any number of points can be provided in the configuration file, as long as they are in an ascending order.

The motor current value and rpm measurements are constantly being read. The electric current estimated by the model for the rpms value being read, is compared against the electric current read by the ADCs. If the value being read is **Motor Current Error Threshold** ampere above the expected value, and remains above it for more than **Motor Current Delay** seconds, a fault detection is triggered. If the last time that an error of this sort was thrown to the output happened more than **Motor Current Error Period** seconds ago, another error is thrown.

The diference being computed can be filtered with a moving average that will use **Position Error Samples** samples for that purpose.

2.3.3 Flowchart

Figure 2.3 depicts the flowchart of how the fault detection method works. The variable *error* represents the difference between the actual motor current being read and the current expected by the piecewise linear model referred above.

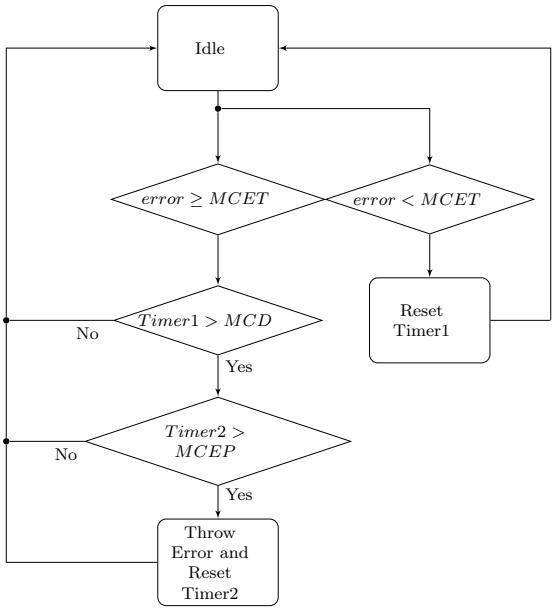

Figure 2.3: Motor current fault detection flowchart.

2.4 SMS Emergency Mechanism

2.4.1 Configuration

Configuration parameters for this mechanism are located in ....

Parameter Name	Acronym	Default	Description

2.4.2 Description

...

2.4.3 Flowchart

Figure ...